IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE: SOCIAL MEDIA ADOLESCENT ADDICTION/PERSONAL INJURY PRODUCTS LIABILITY LITIGATION	)	MDL No. 3047
	)	Case No. 4:22-md-03047-YGR
ALL ACTIONS	)	**JOINT STATEMENT RE: PROTECTIVE ORDER DISPUTES**
	)	Judge: Hon. Yvonne Gonzalez Rogers
	)	Magistrate Judge: Hon. Thomas S. Hixson

Dear Judge Hixson:

Plaintiffs and Defendants have largely reached agreement on a stipulated Protective Order ("PO"), but certain disputed issues remain. The Parties respectfully seek the Court's assistance to resolve their remaining disputes. See CMO No. 5 (Dkt. 164) at 4. The Parties attach the following exhibits to this Joint Statement:

- **Exhibit A** - Plaintiffs' proposed Protective Order with Defendants' proposed additions/deletions in redline;[1]
- **Exhibit B** - Clean version of Plaintiffs' proposed Protective Order;
- **Exhibit C** - Redline comparison between Plaintiffs' proposed Protective Order and this District's Standard Model Protective Order;
- **Exhibit D** - Clean version of Defendants' proposed Protective Order; and
- **Exhibit E** - Redline comparison between Defendants' proposed Protective Order and this District's Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets.

Pursuant to Your Honor's Discovery Standing Order and Civil Local Rule 37-1, the Parties attest that they met and conferred telephonically and exchanged various redlines of each side's proposal before filing this Joint Statement. The parties further attest that they have complied with section 9 of the Northern District of California's Guidelines for Professional Conduct.

The parties would welcome a telephonic conference to discuss these disputed issues if the Court would find it helpful.

[1] Reference to certain paragraphs or pages and lines refers to those in the redline version identifying the Parties' disputed language, which is submitted as Exhibit A to this Joint Statement.

Dated: March 17, 2023

Respectfully submitted,

/s/ Lexi J. Hazam

Lexi J. Hazam
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 BATTERY STREET, 29TH FLOOR
SAN FRANCISCO, CA 94111-3339
Telephone: 415-956-1000
lhazam@lchb.com

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS, LLP
55 CHALLENGER ROAD, 6TH FLOOR
RIDGEFIELD PARK, NJ 07660
Telephone: 973-639-9100
Facsimile: 973-679-8656
cseeger@seegerweiss.com
cayers@seegerweiss.com

Previn Warren
MOTLEY RICE LLC
401 9th Street NW Suite 630
Washington DC 20004
T: 202-386-9610
pwarren@motleyrice.com

Plaintiffs' Co-Lead Counsel

COVINGTON & BURLING LLP

/s/ Ashley M. Simonsen
Ashley M. Simonsen, SBN 275203
COVINGTON & BURLING LLP
1999 Avenue of the Stars
Los Angeles, CA 90067
Telephone: (424) 332-4800
Email: asimonsen@cov.com

Phyllis A. Jones, *pro hac vice*
Paul W. Schmidt, *pro hac vice*
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
Telephone: + 1 (202) 662-6000
Facsimile: + 1 (202) 662-6291
Email: pajones@cov.com
Email: pschmidt@cov.com

Emily Johnson Henn (State Bar. No. 269482)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
Telephone: + 1 (650) 632-4700
Facsimile: +1 (650) 632-4800
Email: ehenn@cov.com

Attorneys for Defendants Meta Platforms, Inc. f/k/a Facebook, Inc.; Facebook Holdings, LLC; Facebook Operations, LLC; Facebook Payments, Inc.; Facebook Technologies, LLC; Instagram, LLC; Siculus, Inc.; and Mark Elliot Zuckerberg

KING & SPALDING LLP

/s/ Geoffrey M. Drake

Geoffrey M. Drake
King & Spalding LLP
1180 Peachtree Street, NE, Suite 1600
Atlanta, GA 30309
Telephone: + 1 (404) 572-4600
Facsimile: + 1 (404) 572-5100
Email: gdrake@kslaw.com

David Mattern
King & Spalding LLP
1700 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: +1 (202) 626-2946
Email: dmattern@kslaw.com

FAEGRE DRINKER LLP

/s/ Andrea Roberts Pierson

Andrea Roberts Pierson
Faegre Drinker LLP
300 N. Meridian Street, Suite 2500
Indianapolis, IN 46204
Telephone: + 1 (317) 237-0300
Facsimile: + 1 (317) 237-1000
Email: andrea.pierson@faegredrinker.com

Amy R. Fiterman
Faegre Drinker LLP
90 South Seventh Street
2200 Wells Fargo Center
Minneapolis, MN 55402
Telephone: +1 (612) 766-7000
Email: amy.fiterman@faegredrinker.com

Attorneys for Defendants TikTok Inc. and ByteDance Inc.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

/s/ John H. Beisner

John H. Beisner (*pro hac vice*)
Skadden, Arps, Slate, Meagher & Flom LLP

1440 New York Avenue, N.W
Washington, D.C. 20005-2111
Telephone: (202) 371-7410
Email: john.beisner@skadden.com

Attorneys for Defendant Snap Inc.

WILLIAMS & CONNOLLY LLP

/s/ Joseph G. Petrosinelli

Joseph G. Petrosinelli
Ashley W. Hardin
Williams & Connoly LLP
680 Maine Avenue, SW
Washington, DC 200024
Telephone: (202) 434-5000
Email: jpetrosinelli@wc.com
Email: ahardin@wc.com

Attorneys for Defendants YouTube, LLC, Google LLC, and Alphabet Inc.

I. PLAINTIFFS' POSITION

Plaintiffs propose a protective order consistent with this District's standard Model Stipulated Protective Order (the "Standard MPO"). Defendants propose to deviate from that standard and instead adopt the District's Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets (the "Trade Secrets MPO")—or in many instances even more restrictive language. These constraints are unwarranted in a mass tort and product liability case like this one, which does not merit an "extremely restrictive type of protective order." *Johnson v. City and County of San Francisco*, 2011 WL 13377688, at *3 (N.D. Cal. Feb. 9, 2011).[2] Such an order would needlessly limit the public's right of access to these proceedings. The Standard MPO is appropriate here, with limited exceptions to account for the fact that Defendants are competitors of one another.[3]

Scope (¶ 3.2). Plaintiffs object to Defendants' proposed language needlessly expanding the Order's scope (*see* Ex. A at 5:16-20), which is not present in either MPO. Defendants seek to designate information as "protected" even if it is *already part of the public domain*, subject to a vague test of whether it constitutes "unsubstantiated media speculation or rumors." That language would invite unnecessary disputes and risk chilling public discourse about the conduct at issue here. Defendants' language is a solution in search of a problem as the Parties have agreed to a proposed sealing order. *See* Proposed Sealing Order (Dkt. 142).

Designation challenges (§ 6). Defendants propose language that deviates from both MPOs by stripping Non-Parties (like the press) of the ability to challenge confidentiality designations, of particular importance here given the strong public interest in the youth mental health crisis. *See, e.g., In re Nat'l Prescription Opiate Litig.*, 927 F.3d 919, 936 (6th Cir. 2019) (noting a "strong presumption in favor of openness of court records"). This is mirrored by their attempt to narrow the definition of "Non-Party" from both MPOs. Ex. A at 3:16-17. Defendants also seek to expand the number of days to seek judicial intervention and to shift the burden of filing motions regarding confidentiality after an arbitrary number of unsuccessful challenges. There is no reason for these deviations from the MPOs. Twenty unsuccessful challenges out of 200 would be a 90% success rate, and thus not indicative of an abuse of process, other than overdesignation by Defendants. Besides, Defendants' conjecture of bad faith does not constitute "certain circumstances" under which the Trade Secrets MPO (¶ 6.3 n.1) says a burden shift "may be appropriate."

Data security (¶ 7.2). Defendants seek to impose a lengthy paragraph on "data security" beyond what is provided for in both model MPOs. Plaintiffs have agreed to the model language (¶ 7.1): "Protected material must be stored and maintained by a Receiving Party at a location and in a secure manner that ensures that access is limited to the persons authorized under this Order." Defendants have not provided any justification for a deviation from this model language. Moreover, Defendants' additional proposed restrictions concerning the "standard industry practices" of a Party's data security storage are unworkably vague.

---

[2] In the cases Defendants cite, *infra* at 3, the parties agreed to the Trade Secrets MPO.

[3] The Parties have agreed that source code will be dealt with in a separate order, *see* CMS (Dkt. 143) at 18, which may contemplate additional restrictions for such material.

Restrictions on experts to review confidential material (¶ 2.9 (expert definition); ¶ 7.7 (disclosure to experts)). Plaintiffs object to Defendants' proposed definition of "Expert" to exclude any "past" employee "of a Party or a Party's competitor." While the Standard MPO has no such restriction, to address Defendants' concern that they are competitors with one another, Plaintiffs agreed to a definition that excludes a Defendant's *current* employees from access to other Defendants' highly confidential material. That resolves Defendants' vaguely stated concern of "competitive harms" from disclosure. The purpose of the "highly confidential—competitor" designation is to protect against other *parties* seeing material they would otherwise have access to (not non-parties without access). Coupled with the disclosure requirements they seek, Defendants' language would severely limit Plaintiffs' ability to retain qualified experts by virtue of past employment at any of the Defendant platforms *or any* other competitors. Plaintiffs' less onerous approach has been adopted in other cases where a social media company's software is at issue, including that of a Defendant here. *See In re Facebook, Inc. Consumer Privacy User Profile Litig.*, No. 18-MD-2843-VC (N.D. Cal. 2018), ECF 122 ¶ 2.6.

Plaintiffs also object to Meta, YouTube, and TikTok's proposal that the Parties not be permitted to disclose highly confidential material to retained experts without first identifying the expert to the Designating Party and providing extensive information about the expert (including information that goes beyond the Trade Secrets MPO). The Standard MPO contains no such requirement, which would "effectively allow the Defense to vet Plaintiffs' expert, eviscerate the work product privilege regarding any expert they may choose not to use, and require premature disclosure of the identity of any expert(s)." *Johnson*, 2011 WL 13377688, at *2. The Court should not require Plaintiffs "to disclose in advance the identity of anyone they might consult" because this "potentially invades the attorney work product doctrine and removes [their] ability to have non-disclosed consulting experts." *Todd v. Tempur-Sealy Int'l, Inc.*, 2015 WL 433481, at *4 (N.D. Cal. Feb. 2, 2015). The Court should adopt the Standard MPO on this issue.[4]

Disclosure of "HIGHLY CONFIDENTIAL (COMPETITOR)" Protected Material (¶ 7.5). Plaintiffs object to Defendants' proposed language barring disclosure of "HIGHLY CONFIDENTIAL (COMPETITOR)" Protected Material to certain witnesses during depositions, impeding their efficiency. Plaintiffs' proposed language is sufficiently protective: it allows deposition witnesses to view "HIGHLY CONFIDENTIAL (COMPETITOR)" Protected Material where reasonably necessary and where the witness signs the "Acknowledgment and Agreement to Be Bound" (Exhibit A) to the Protective Order, while prohibiting disclosure to individual Plaintiffs or officers, directors, and employees of other Defendants, including House Counsel, who did not author, receive, or are not otherwise aware or in possession of the document.

Export controls (¶ 12.4). Plaintiffs object to Defendants' proposed "Export Controls" provision, which is not in the Standard MPO. Defendants' bare citation to language from the Export Administration Regulations does *not* establish that such materials are at issue in this case or that the regulations will apply.[5] Moreover, Defendants' language would prohibit the viewing

[4] Plaintiffs' position is closer to Snap's proposal permitting disclosure of highly confidential material without these disclosure requirements "as long as the Expert is not a *current* officer, director, or employee of a competitor of a Party or anticipated to become one." Ex. A at 16:2–3.

[5] Defendants' EAR citation simply begs the question: 15 C.F.R. § 772.1 defines "technology," but does not address when and under what circumstances "technology" is export-controlled. The

of *any* designated material outside of the U.S., *irrespective of* whether it is subject to export control.[6] The Court should not accept Defendants' use of the canard of export laws to impose such onerous obligations on Plaintiffs and their experts. Notably, the cases Defendants cite are inapposite as they are all patent cases. In addition, *VideoShare* permitted the viewing of highly confidential material (other than source code) "through electronic means outside the territorial limits of the United States," No. 1:13-cv-991 (D. Del. Mar. 4, 2015), ECF 37 at 20, and the defendants in *Dynamic Data* indicated that they could simply agree to allow overseas use of the subject material. No. 2:18-cv-459 (E.D. Tex. Apr. 30, 2019), ECF 84 at 17.

Source code. Plaintiffs object to Defendants' inclusion of a source code definition (¶ 2.22). The Parties agreed that source code would be governed by separate proposed order, and no further productions will be made pending motions to dismiss. Thus Defendants' definition—which is different from and broader than that in the Trade Secrets MPO—is premature.

II. DEFENDANTS' POSITION

This Court should begin with the model N.D. Cal. PO for "litigation involving . . . highly sensitive confidential information and/or trade secrets" ("HC Model"). Defendants are four competitor technology companies. Plaintiffs' claims implicate not only highly confidential source code, but also Highly Confidential (Competitor) ("HCC") information like algorithms, business strategies, and other sensitive information that would put Defendants at a disadvantage if disclosed. The HC model is the only model that includes a highly confidential designation and related provisions designed to protect this kind of competitive information and provides "presumptively reasonable conditions" for discovery. *Corley v. Google, Inc.*, 2016 WL 3421402, at *1 (N.D. Cal. June 22, 2016). This Court routinely follows the HC Model in cases like this one. *E.g.*, *In re Apple iPhone Antitrust Litig.*, No. 4:19-cv-3074 (N.D. Cal. Jan. 9, 2020), ECF #85; *Rumble, Inc. v. Google LLC*, No. 4:21-cv-229 (N.D. Cal. Oct. 27, 2022), ECF #76.

I. Following the HC Model resolves much of the dispute. Defendants' proposal largely follows the HC Model as-is or with minor clarifications (most of which appear in similar POs). Defendants seek adoption of the following HC Model provisions, which Plaintiffs oppose:

- Employees as Experts (§ 2.9). All Defendants (including Snap) agree that, to protect the designating party from competitive harms, *past*, current, and future employees of a party or competitor should not receive Confidential or HCC material. *Corley*, 2016 WL 3421402, at *2 (courts have "repeatedly ruled" that hiring past employee experts is "improper").

- Public Domain (§ 3.2): To avoid circumvention of court-ordered protections, Defendants would clarify that information (including unsubstantiated media speculations/rumors) confirmed only through the review of protected material or violation of another court's order is not in the public domain. *See United States v. Barbeito*, 2010 WL 1439510, at *1 (S.D. W. Va.

---

fact that information may meet the definition of "technology" doesn't mean that its release requires controls. Indeed, Plaintiffs understand that the vast majority of discovery here, apart from potentially source code, would not be subject to heightened classification under the EAR (and Defendants notably have not actually identified anything that is or will be).

[6] Defendants' proposal thereby imposes restrictions beyond even the *optional* export control provision in the Trade Secrets MPO, while relieving Defendants of the obligations therein.

Apr. 8, 2010); *In re Facebook*, 2021 WL 3209711, at *4; *Ameziane v. Obama*, 699 F.3d 488, 498 (D.C. Cir. 2012) ("Why honor confidentiality restrictions . . . if ignoring them will be rewarded?").

- Procedure for Challenging Confidentiality (§ 6.3): As contemplated in footnote 1 of the HC Model, Defendants seek to shift the burden of filing a motion to the challenging party following unsuccessful challenges to 20 designations. This shifting prevents asymmetrical abuse of process, because Defendants will produce the most discovery and Plaintiffs' cost of challenges is low. Given the volume of discovery, Defendants seek 30 days to oppose challenges.

- Data Security (§ 7.2): The HC Model requires storage of data in a "secure manner." Because Plaintiffs' claims implicate discovery of Defendants' highly guarded competitive information, and because such "ESI productions . . . can be ripe targets for corporate espionage and data breach," Sedona Principles (3d Ed.), 19 Sedona Conf. J. 1, 179 n.147 (2018), Defendants seek information security "consistent with standard industry practices." A party whose systems do not meet industry standards can easily comply by using a reputable eDiscovery vendor.

- Limitations on Disclosure of HCC Material (§ 7.5): HCC material should not be disseminated to deponents who did not author or receive the materials or to experts who are not properly disclosed (§ 7.7). Contrary to the HC Model, Plaintiffs seek to make the list of individuals eligible to receive Confidential and HCC material virtually indistinguishable.

- Export Control (§ 12.4): Section 14.3 of the HC Model contemplates export control restrictions, because Defendants legally cannot permit or enable Plaintiffs to access their controlled "technical data" outside the U.S. or provide that data to non-U.S. persons, without ensuring compliance with 15 C.F.R. §§ 730–74; *cf. id.* § 764.3 (penalties). Because Plaintiffs' allegations directly target algorithms and technical design features, discovery will involve "technical data"—which includes not only source code, but also "engineering designs and specifications" and "manuals or documentation." *Id.* § 772.1. Defendants propose language that courts have substantively approved in other cases. *See, e.g.*, *Virentem Ventures v. YouTube*, No. 1:18-cv-917 (D. Del.), ECF #85 (approving after dispute, ECF #80); *VideoShare v Viddler*, No. 13-cv-991, ECF #37 (D. Del.); *Dynamic Data Techs., LLC v. Samsung Elecs. Co.*, No. 2:18-cv-459 (E.D. Tex.), ECF #84 (approving departure from N.D. Cal. Model over dispute, ECF #64).

II. Defendants also would delete allowances for unlimited non-party confidentiality designation challenges (§§ 2.13, 6.1). Given the volume of anticipated discovery, such challenges risk overburdening the Court and the parties. Multiple approved POs exclude this HC Model provision. *E.g.*, *Newman v. Google LLC*, No. 3:22-cv-2799 (N.D. Cal. May 11, 2022), ECF #19; *Davis v. Pinterest, Inc.*, No. 4:19-cv-7650 (N.D. Cal. 2019), ECF #70.

III. Finally, Defendants seek guidance on three issues over which they disagree:

- In-House Counsel ("IHC") Access to HC Material (§§ 2.3, 2.6, 7.5(b), 7.8, 8): **Snap, Meta, and YouTube** seek to adopt the HC Model's IHC provisions, which permit up to two IHC not "involved in Competitive Decision-Making" to access HCC information via a secure, read-only platform (a precaution beyond the HC Model). Courts consistently recognize the need for and approve IHC provisions for litigation IHCs who "are not competitive decisionmakers." *E.g.*, *MedImpact Healthcare Sys., Inc. v. IQVIA Inc.*, 2021 WL 389820, at *4 (S.D. Cal. Feb. 4,

2021) (overruling objection); *Alza Corp. v. Impax Labs., Inc.*, 2004 WL 7339748, at *2–4 (N.D. Cal. June 21, 2004) ("[i]n-house counsel are not second-class lawyers who cannot be trusted with sensitive information"); *Newmark Realty Cap., Inc. v. BGC Partners, Inc.*, 2017 WL 2591842, at *1 (N.D. Cal. June 15, 2017) (rejecting competitor objection). **TikTok** believes that the Court should use the default language in the HC Model, which grants IHC access to confidential material but reserves trade secrets for outside counsel. Defendants are direct competitors (harm to TikTok by disclosure: high) and are represented by outside counsel (harm by no IHC access: "nonexistent"). *Adobe Sys. v. Davachi*, 2011 WL 2610170, *4 (N.D. Cal. 2011); *Pinterest v. Pintrips*, 2014 WL 5364263, at *3 (N.D. Cal. 2014). The other defendants' IHC do not need access to TikTok's HCC, and their desire "to closely supervise [] outside counsel" by reviewing filings "is insufficient." *Id.* Finally, the definition of "competitive decision-making" is too broad in that it excludes all "legal advice." *Brown Bag v. Symantec Corp.*, 960 F.2d 1465, 1471 (9th Cir. 1992) (IHC restrictions aim to prevent "legal advice" about competitors).

- Disclosure to Liability Insurers (§§ 2.12, 7.3(b), 7.8, 8, 13.2): **Snap, Meta, and YouTube** would allow liability insurers to receive confidential information, with access limited to necessary representatives after notice and an opportunity to object. Such provisions are routine. *E.g., In re Air Crash at S.F. on July 6, 2013*, No. 4:13-md-2497 (N.D. Cal. Aug. 11, 2014), ECF #156; *In re McKinsey & Co. Nat'l Prescription Opiate Consultant Litig.*, No. 3:21-md-2996 (N.D. Cal. Sept. 21, 2021), ECF #258. Insurers could otherwise assert they lack sufficient information to cover a claim. **TikTok** opposes this provision: it is not included in the HC Model, and *Air Crash* and *McKinsey* involved unopposed/stipulated protective orders. To TikTok's knowledge, no court has adopted such a provision over a party's objection. *Tylor v. Hawaiian Springs*, 2019 WL 13160076, at *3 (D. Hi. 2019) ("This insurer is not a party to this lawsuit, and as such it is not entitled to information designated confidential"). The other Defendants have articulated no reason why their carriers need access to TikTok's confidential information or to retain it indefinitely.

- Expert Disclosures (§ 7.7): **Meta, YouTube, and TikTok** would follow the HC Model for expert disclosures, which requires a receiving party to disclose information about an expert before providing HCC, and also requires disclosure of an expert's patents (or applications). *E.g., Sentius Int'l, LLC v. Apple, Inc.*, No. 4:20-cv-477-YGR (N.D. Cal. Nov. 5, 2020), ECF #73. "A party should have an opportunity to vet someone who is going to have access to their 'extremely sensitive' confidential information" and "should not have to rely on an opponent's expert's self-evaluation of conflicts." *In re Google Assistant Priv. Litig.*, 2020 WL 4698810, at *2 (N.D. Cal. Aug. 13, 2020) (rejecting *Todd*). **Snap** would adopt HC Model footnote 7. Given the novel scientific and legal issues, the parties are likely to rely on a wide range of consulting experts. Forcing premature disclosure of experts would allow parties improperly to discern and vet each other's strategies prior to Rule 26 expert disclosures from the expert's area of expertise and the topics on which they are being consulted; and could result in a privilege waiver. *Todd*, 2015 WL 1022886, at *3; *Corley*, 2016 WL 3421402 at *3-4 (approving PO allowing withholding of non-testifying experts). Comparable POs do not require expert disclosure prior to the Rule 26 timeline. *E.g. In re Apple iPhone*, *supra*; PO, *In re Facebook*, No. 3:18-MD-2843 (N.D. Cal. Aug. 17, 2018).

ATTESTATION

I, Lexi J. Hazam, hereby attest, pursuant to N.D. Cal. Civil L.R. 5-1, that the concurrence to the filing of this document has been obtained from each signatory hereto.

DATED: March 17, 2023 By: */s/Lexi. J. Hazam*
Lexi J. Hazam